МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

Радіотехнічний факультет

Кафедра прикладної радіоелектроніки

ЗВІТ

З ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Виконав:

Студент 3 курсу, групи РІ-п01

Фоменчук Б.А.

(Прізвище І.П.)
Підпис

Звіт прийняв:

Новосад А.А.

(Прізвище І.П. Підпис керівника диплому від кафедри)

«27» 05 2023 р.

Шульга А.В.

«____» _____2023 р.

Київ – 2023 р.

Зміст

1. Вступ

Сучасні умови, в яких ми вимушені жити, дуже змінилися з початком епідемії COVID-19, цифровізації, можливостей для віддаленої роботи. В наші дні вже нікого не здивуєш точкою доступа WiFi у парку, кафе, бібліотеці, спортзалі, лікарні, аеропорту, готелі. Це скоріше норма життя, яка покликана зробити життя людей більш зручним, дати їм можливість отримувати доступ до інформації, зв'язку, месенджерів, інших веб-ресурсів, мати можливість працювати або вчитися, всього лише маючи при собі телефон або ноутбук, підключившись до будь-якої з доступних точок WiFi. Але під виглядом цієї зручності криється багато "підводних каменів", які можуть становити загрозу не тільки персональним даним користувача (паролі, номери карток, повідомлення і т.д.), але і можуть розповсюджувати шкідливе програмне забезпечення, яке потенційно може може нашкодити підприємству, компанії, навчальному або іншій людині, з якими пов'язаний(а) даний користувач(ка).

Публічні мережі дуже зручні для користування, так як надають можливість отримувати доступ до інтернету практично з будь-якого місця у будь-який час. Але, зважаючи на те, що ці мережі налаштовуються і контролюються невідомими користувачу особами, а також часто є відкритими, тобто не потребують аутентифікації та авторизації і будь-хто може приєднатися до подібної мережі і використовувати особливості і вразливості мережі, подібні мережі не можна вважати безпечними. Саме тому дуже важливим є забезпечення безпечного доступу до інтернету у

даних мережах. Одним з таких способів є відмежування користувача від потенційно небезпечної, тобто відкритої, мережі пристроєм, який би логічно розташовувався між користувачем і публічною мережею, був би одночасно клієнтом для публічної мережі і точкою доступу для користувача, утворюючи при цьому “довірчу” підмережу для пристроїв користувача.

2. Аналіз існуючих рішень

На рис. 2.1 зображений GL.iNet (Slate AX) WiFi 6 Travel Router

Рисунок 2.1– Портативний роутер компанії GL.iNet

Ключові характеристики:

- 1,800Мб/с сумарна пропускна здатність
- Два порти LAN

- ➓ Передвстановлені VPN клієнт і Cloudflare шифрування
- ➓ Працює як WiFi повторювач
- ➓ Передвстановлений AdGuard Home

Slate AX — це маршрутизатор WiFi 6, що означає, що він підтримує останню версію WiFi. Звичайно, він все ще сумісний зі старими версіями Wi-Fi, такими як 802.11c/g/ac. З підключенням WiFi 6 ви можете скористатися підтримкою MU-MIMO.

Роутер дозволяє отримати 600 Мбіт/с пропускної здатності на каналі 2,4 ГГц і 1200 Мбіт/с на каналі 5 ГГц. У сукупності це становить 1800 Мбіт/с пропускної здатності. Порти LAN, тим часом, забезпечують стандартні значення 10/100/1000.

Апаратне забезпечення — це ще не все, що ви отримуєте. Slate AX поставляється з уже встановленими OpenVPN і WireGuard. Це популярні служби VPN, які зберігають вашу особисту інформацію під час перегляду. Швидкість OpenVPN обмежена 120 Мбіт/с, а WireGuard підтримує 550 Мбіт/с. Крім того, маршрутизатор підтримує понад 30 інших служб VPN. Ще краще, усі ваші з’єднання зашифровано Cloudflare. Це дає їм такий самий рівень безпеки, як веб-сайт «https».

На рис. 2.2 зображений NewQ Filehub AC750 Wireless Travel Router

Рисунок 2.2– Портативний роутер компанії NewQ

Ключові характеристики:

- ➓ 733 Мб/с максимальна пропускна здатність
- ➓ 6,500 мАг ємність вбудованого акумулятора
- ➓ Три режими роботи: точка доступу, роутер, міст

Індикатори повідомляють, коли ви підключені до Інтернету, коли Wi-Fi активний, а також інші важливі дані. На передній панелі є слот Micro SD для мережевого зберігання. Порти розташовані на лівій стороні корпусу. На задній панелі є порт USB Type-A для зберігання, також порт живлення USB Type-C. Спереду знаходиться порт WAN.

Мережеві можливості та додаткові можливості:

AC750 має пропускну здатність 300 Мбіт/с на каналі 2,4 ГГц і 433 Мбіт/с на каналі 5 ГГц. Це загалом 733 Мбіт/с, що трохи повільно, але все ж достатньо швидко, щоб бути корисним. Його можна використовувати як точку доступу, маршрутизатор або міст.

На рис. 2.3 зображений TP-Link Nano Wireless Travel Router

Рисунок 2.3 – Портативний роутер компанії TP-Link

Ключові характеристики:

- ➓ 733 Мб/с максимальна пропускна здатність
- ➓ Один Ethernet порт з подвійним функціоналом LAN/WAN
- ➓ Доступна ціна

Коли користувачу потрібен лише базовий Wi-Fi із прийнятною швидкістю, це може бути ідеальним вибором.

Маршрутизатор Nano Travel Router має пропускну здатність 733 Мб/с. Однак він також підтримує підключення Ethernet. Також слід мати на увазі, що тут є компроміс. Якщо користувач підключить комп’ютер до порту Ethernet, йому доведеться підключити маршрутизатор до мережі через WiFi. Якщо користувач підключить маршрутизатор до модему або розетки, він зможете підключити комп’ютер лише через WiFi.

3. Безпековий функціонал звичайного WiFi роутера і аналіз його вразливостей

3.1 Типові конфігурації WiFi роутерів

Звичайні користувачі не мають достатніх технічних знань і навичок для налаштування WiFi роутерів, тому, купуючи подібні девайси, користувачі зазвичай використовують стандартні налаштування, тобто логін і пароль для підключення. WiFi роутери, які використовуються, як точки доступу публічних мереж зазвичай конфігуруються спеціалістами і мають більш складні і гнучкі налаштування, серед яких можуть бути налаштування firewall, більш складні методи аутентифікації (WPA2, WPA3), системи виявлення і попередження вторгнення. Але той факт, що точки доступу налаштовуються сторонніми людьми і безпека даних користувача залежить від когось, вже викликає сумніви і змушує задуматися над раціональністю використання подібних мереж.

3.2. Методи шифрування і аутентифікації

Є чотири варіанти шифрування. Зрозуміло, не рахуючи "Open" (Ні захисту).

- **WEP** (Wired Equivalent Privacy) - застарілий і небезпечний метод перевірки автентичності. Це перший і не дуже вдалий метод захисту. Зловмисники без проблем отримують доступ до бездротових мереж, які захищені за допомогою WEP. Не потрібно встановлювати цей режим в налаштуваннях свого роутера, хоч він там і присутній (не завжди).
- **WPA** (Wi-Fi Protected Access) - надійний і сучасний тип безпеки. Максимальна сумісність з усіма пристроями і операційними системами.
- **WPA2** - нова, допрацьована і більш надійна версія WPA. Є підтримка шифрування AES CCMP.

WPA / WPA2 може бути двох видів:

- **WPA / WPA2 - Personal (PSK)** - це звичайний спосіб аутентифікації. Коли потрібно задати тільки пароль (ключ) і потім використовувати його для підключення до Wi-Fi мережі. Використовується один пароль для всіх пристроїв. Сам пароль зберігається на пристроях. Де його при необхідності можна подивитися, чи змінити. Рекомендується використовувати саме цей варіант.
- **WPA / WPA2 - Enterprise** - більш складний метод, який використовується в основному для захисту бездротових мереж в офісах і різних закладах. Дозволяє забезпечити більш високий рівень захисту. Використовується тільки в тому випадку, коли для авторизації пристроїв встановлений RADIUS-сервер (який видає паролі)
- **Wi-Fi Protected Access 3 (WPA3)**

Оскільки ключова вразливість ховалася в чотиристоронньому рукостисканні, WPA3 додалася обов'язкова підтримка більш надійного методу з'єднання — SEA, також відомого як Dragonfly. Технологія SEA (Simultaneous Authentication of Equals) вже застосовувалася в mesh-мережах та описана у стандарті IEEE 802.11s. Вона заснована на протоколі обміну ключами Діффі-Хеллмана з використанням кінцевих циклічних груп. SEA відноситься до протоколів типу PAKE і надає інтерактивний метод, відповідно до якого дві і більше сторони встановлюють криптографічні ключі, що базуються на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який одержує кожна зі сторін для автентифікації з'єднання, вибирається на основі інформації з пароля, ключів та MAC-адрес

обох сторін. Якщо ключ однієї зі сторін виявиться скомпрометований, це не спричинить компрометацію ключа сесії. І навіть дізнавшись пароль, атакуючий не зможе розшифрувати пакети. Ще одним нововведенням WPA3 є підтримка PMF (Protected Management Frames) для контролю за цілісністю трафіку.

Як і в WPA2, в WPA3 передбачено два режими роботи: WPA3-Personal та WPA3-Enterprise.

- WPA3-Personal забезпечить надійний захист, особливо якщо користувач поставив стійкий пароль, який не можна отримати словниковим перебором. Але якщо пароль не зовсім тривіальний, то має допомогти нове обмеження на кількість спроб автентифікації в рамках рукостискання. Також обмеження не дозволить підбирати пароль у офлайновому режимі. Замість ключа PSK WPA3 реалізована технологія SEA.
- WPA3-Enterprise передбачає шифрування на основі щонайменше 192-розрядних ключів, що відповідають вимогам CNSA (вони вироблені комітетом NSS для захисту урядових, військових та промислових мереж). Для автентифікованого шифрування рекомендовано застосування 256-розрядних ключів GCMP-256, для передачі та підтвердження ключів використовується HMAC з хешами SHA-384, для узгодження ключів та автентифікації – ECDH та ECDSA з 384-розрядними еліптичними кривими, для захисту цілей GMAC-256[4].

У Wi-Fi мережах існують різні протоколи аутентифікації, які використовуються для перевірки і підтвердження ідентичності

користувача, що намагається підключитися до бездротової мережі. Основні протоколи аутентифікації Wi-Fi включають:

PSK (Pre-Shared Key): Це найпростіший метод аутентифікації, який використовується в більшості домашніх бездротових мереж. Користувачі вводять спільний пароль або ключ, який заздалегідь встановлений на точці доступу та пристрої, що підключаються. Цей пароль використовується для шифрування трафіку між пристроями.

802.1X / EAP (Extensible Authentication Protocol): Цей протокол використовується в підприємницьких мережах та вимагає сервера аутентифікації для перевірки ідентичності користувача. Користувачі вводять свої індивідуальні облікові дані (логін та пароль) або використовують інші методи аутентифікації, такі як сертифікати або токени.

WPS (Wi-Fi Protected Setup): WPS - це метод спрощеної аутентифікації, який дозволяє користувачам підключати нові пристрої до мережі за допомогою кнопки WPS або ПІН-коду. Використовуючи WPS, пристрій може автоматично отримати необхідні облікові дані для підключення до мережі.

Captive Portal: Цей метод аутентифікації використовується в громадських мережах, таких як кав'ярні або аеропорти. При спробі підключитися до мережі, користувач переадресовується на сторінку аутентифікації, де йому потрібно ввести логін та пароль або пройти інший вид ідентифікації (наприклад, соціальні медіа).

Ці протоколи аутентифікації використовуються для забезпечення безпеки і

контролю доступу до Wi-Fi мереж. Вибір протоколу залежить від типу мережі (домашня, підприємницька, громадська) і вимог безпеки, що ставляться до мережі.

3.3 Інструменти і методи злому WiFi мереж

Розглянемо методи злому WPA/WPA2 PSK так як даний спосіб аутентифікації та шифрування є найбільш поширеним серед звичайних користувачів і публічних мереж. Типова стратегія злому WiFi мережі зазвичай складається з наступних кроків:

1. Розвідка з метою отримання інформації про мережу(частота, канал, потужність сигналу), типу шифрування і аутентифікації, MAC адреси точки доступу і її клієнтів.
2. Отримання паролю точки доступу (якщо мережа не відкрита)
3. Проведення Man-in-the-Middle атаки, яка дозволяє зловмиснику прикинутися точкою доступу для клієнта і клієнтом для точки доступу, після чого увесь трафік від клієнта в інтернет буде проходити через пристрій зловмисника
4. Підміна DNS сервера, підміна HTTPS запитів на HTTP для переадресування запитів клієнта на сторонні ресурси з метою отримання конфіденційних даних або зараженням пристрою клієнта файлами зі шкідливим ПЗ [5].

Для подібного роду атак існують спеціально розроблені інструменти, які зручні і не потребують глибоких знань для їх використання, що дозволяє проводити такі атаки майже будь кому, хто має базові знання використання комп’ютерів, що робить такі атаки ще більш масовими.

Найбільш популярним типом атаки з метою отримання доступу до WiFi мережі з WPA2 PSK є так звана атака по словнику.

WPA/WPA2 PSK працює так: він випливає з ключа попередньої сесії, яка називається Pairwise Transient Key (PTK). PTK, у свою чергу, використовує Pre-Shared Key і п'ять інших параметрів - SSID, Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адреса точки доступу) і Suppliant MAC-address (MAC-адреса wifi -Клієнта). Цей ключ надалі використовує шифрування між точкою доступу (AP) та WiFi-клієнтом. Зловмисник, який у цей момент прослуховує ефір, може перехопити всі п'ять параметрів. Єдиною річчю, якою не володіє лиходій це – Pre-Shared key. Pre-Shared key виходить завдяки використанню парольної фрази WPA-PSK, яку надсилає користувач, разом із SSID. Комбінація цих двох параметрів пересилається через Password Based Key Derivation Function (PBKDF2), яка виводить 256-bit' загальний ключ. У звичайній WPA/WPA2-PSK-атаці за словником, зловмисник буде використовувати ПЗ, яке виводить 256-бітний Pre-Shared Key для кожної парольної фрази і буде використовувати її з іншими параметрами, які були описані у створенні PTK. PTK використовуватиметься для перевірки Message Integrity Check (MIC) в одному з пакетів handshake. Якщо вони співпадуть, то парольна фраза у словнику буде правильною. При цьому використовуються вразливості протоколу аутентифікації користувачів - відкрита передача ANonce, SNonce, MAC-адреси точки доступу та MAC-адреси WiFi-клієнта. Якщо при відтворенні алгоритму аутентифікації відбудеться «успішна авторизація користувача», то вибраний зі словника пароль є дійсним і атака

призвела до успішного злому мережі. Комбінаторна складність відновлення паролю з хеша означає, що зловмисник повинен спробувати всі можливі комбінації символів паролю і обчислити хеш для кожної комбінації, а потім порівняти отриманий хеш зі збереженим хешем для зламу паролю. Збільшення довжини паролю та використання складніших символів (букв верхнього та нижнього регістрів, цифр, спеціальних символів) значно ускладнюють комбінаторну атаку на пароль. Кожне додаткове символ в паролі збільшує кількість можливих комбінацій, що потрібно перебрати. Наприклад, для паролю довжиною 8 символів, що складаються тільки з малих літер англійського алфавіту (26 символів), комбінаторна складність становить 26^8, що приблизно дорівнює 208 мільярдам можливих комбінацій. Це вимагає значних обчислювальних ресурсів і тривалого часу для перебору всіх комбінацій. Враховуючи це, для забезпечення безпеки паролю рекомендується використовувати довгі паролі (зазвичай не менше 12 символів) з використанням різноманітних символів і регулярно їх змінювати. Це зробить процес відновлення паролю з хеша надзвичайно складним і майже неможливим для зловмисників.

На рис. 3.1 зображена схема обміну ключами і формування ключа шифрування даних між точкою доступу і станцією.

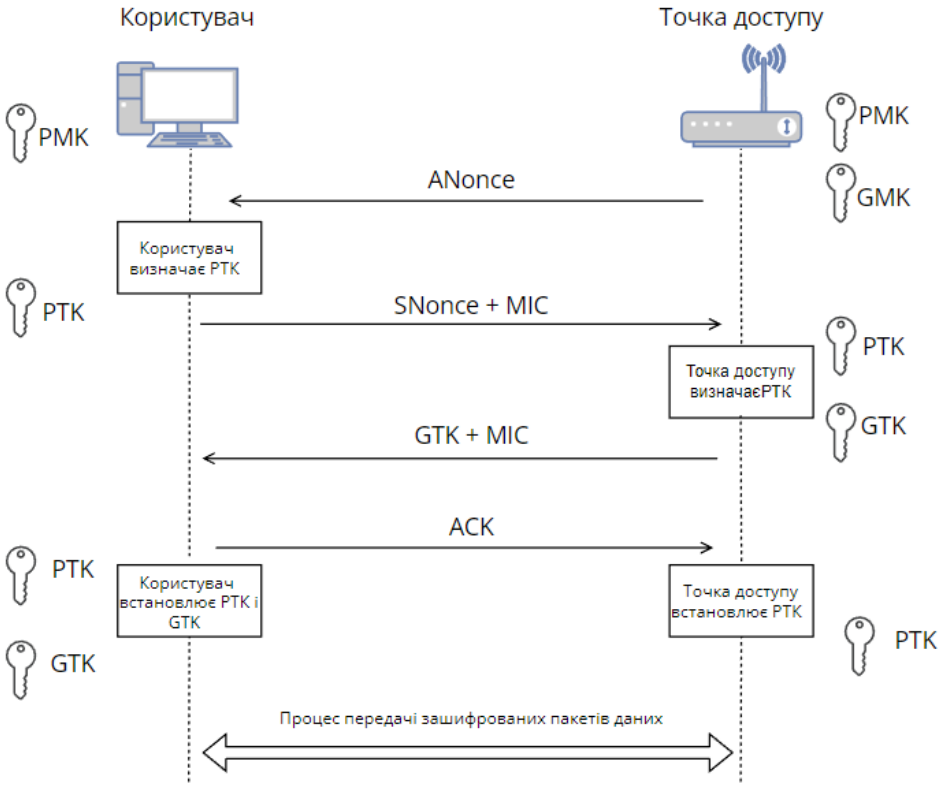

Рисунок 3.1– Схема 4-кратного рукостискання

Нижче наведено визначення різних типів ключів, які використовуються при 4-кратному рукостисканні.

PTK (парний перехідний ключ):

Попарний тимчасовий ключ використовується для шифрування всього одноадресного трафіку між клієнтською станцією та точкою доступу. PTK є унікальним між клієнтською станцією та точкою доступу. Щоб створити PTK, клієнтському пристрою та точці доступу потрібна така інформація.

PTK = PRF (PMK + ANonce + SNonce + MAC (AA) + MAC (SA))

ANonce — випадкове число, згенероване точкою доступу (автентифікатором), SNonce — випадкове число, згенероване клієнтським пристроєм (заявником). MAC-адреси запитувача (клієнтського пристрою) і

MAC-адреси автентифікатора (точки доступу). PRF — це псевдовипадкова функція, яка застосовується до всіх вхідних даних.

PTK залежить від іншого ключа високого рівня PMK (парний головний ключ), який обговорюється нижче.

GTK (тимчасовий ключ групи):

Груповий тимчасовий ключ використовується для шифрування всього широкомовного та багатоадресного трафіку між точкою доступу та кількома клієнтськими пристроями. GTK — це ключ, який спільно використовується між усіма клієнтськими пристроями, пов'язаними з 1 точкою доступу. Для кожної точки доступу буде окремий GTK, який буде спільно використовуватися між пов'язаними пристроями.

GTK залежить від іншого ключа високого рівня GMK (головний ключ групи), який обговорюється нижче.

PMK (парний головний ключ):

Що таке PMK і навіщо він потрібен? Тепер ми знаємо, що таке PTK і GTK. PTK генерується за допомогою PMK. Як ми обговорювали вище, щоб створити PTK, нам потрібні такі вхідні дані.

PTK = PRF (PMK + ANonce + SNonce + MAC (AA) + MAC (SA))

Попарний майстер — це ключ, згенерований із головного сеансового ключа (MSK). У випадку WPA2/PSK, коли пристрій автентифікується за допомогою точки доступу, PSK стає PMK.

Пам'ятаємо, що PMK знаходиться на всіх станціях, як у точках доступу, так і на клієнтських пристроях, тому нам не потрібно ділитися цією інформацією. Ми використовуємо цю інформацію для створення PTK, який

використовується для одноадресного шифрування даних.

GMK (Груповий головний ключ):

Головний ключ групи використовується в 4-сторонньому рукостисканні для створення GTK, описаного вище. GTK генерується на кожній точці доступу та надається спільно з пристроями, підключеними до цієї точки доступу.

MSK (головний сеансовий ключ):

Головний сеанс — це перший ключ, який генерується або з 802.1X/EAP, або походить від автентифікації PSK.

Ще одним методом злому WPA2 PSK аутентифікації і шифрування є так звана атака CRACK (Key Retranslation Attack).
Атака використовує вразливість WPA2 PSK яка дозволяє повторно встановлювати один і той самий криптографічний nons(псевдовипадкове число) на третьому кроці в процедурі відкриття сеансу (так зване рукостискання) за протоколом WPA2. Завдяки цьому зловмисник має можливість здійснити криптоаналіз та встановити сеансовий ключ. Таким чином, зловмисник може прослуховувати дані, а в деяких випадках, навіть підробляти дані, що передаються між клієнтом та точкою доступу [5].

Є декілька найбільш популярних інструментів, які дозволяють моніторити трафік, перехоплювати пакети, здійснювати різні типи атак і зламувати паролі, не обмежуючись WiFi мережами:

⑩ Aircrack-ng

Aircrack-ng — це повний набір інструментів для оцінки безпеки мережі WiFi.Він фокусується на різних сферах безпеки WiFi:

Моніторинг: захоплення пакетів і експорт даних у текстові файли для

подальшої обробки інструментами сторонніх розробників

Атака: повторні атаки, деавтентифікація, фальшиві точки доступу та інші за допомогою введення пакетів

Тестування: перевірка можливостей карт WiFi та драйвера (захоплення та впровадження)

Злом: WEP і WPA PSK (WPA 1 і 2) [1].

⑩ John the Ripper

Вільна програма, призначена для відновлення паролів за їхніми хешами. Основне призначення програми – аудит слабких паролів у UNIX системах шляхом перебору можливих варіантів. ПЗ JtR здатне створювати словники будь-якої складності, а також витягувати хеш із файлу.

⑩ hashcat

Найшвидша та найдосконаліша у світі програма для відновлення паролів з хешів[2].

⑩ wifite

Це інструмент для аудиту бездротових мереж, зашифрованих WEP або WPA. Для виконання аудиту використовуються інструменти aircrack-ng, pyrit, reaver, tshark.

Цей інструмент можна налаштувати для автоматизації за допомогою лише кількох аргументів, і його можна довіряти працювати без нагляду.

⑩ Airgeddon

airgeddon — це обгортка сторонніх інструментів, керована з меню, для аудиту бездротових мереж із багатьма функціями.

⑩ Kismet

Kismet — це сніффер із відкритим кодом, wardriver та інструмент захоплення пакетів для Wi-Fi, Bluetooth, BTLE, бездротових пристроїв, літаків, вимірювачів потужності, Zigbee тощо [3].

У якості типового прикладу злому і демонстрації його простоти нижче наведено покрокова демонстрація цього процесу, використовуючи aircrack-ng, який працює за наступним алгоритмом: за допомогою попередніх спільних ключів клієнт і точка доступу встановлюють ключовий матеріал, який буде використовуватися для їх зв'язку на початку, коли клієнт вперше зв'язується з точкою доступу. Між клієнтом і точкою доступу відбувається чотиристоронне рукостискання. airodump-ng може зафіксувати це чотиристоронне рукостискання. Використовуючи дані зі списку слів (словника), aircrack-ng дублює чотиристоронне рукостискання, щоб визначити, чи відповідає певний запис у списку слів результатам чотиристоронього рукостискання. Якщо так, це означає, що попередній спільний ключ успішно ідентифіковано.

1. Підготовка тестового середовища

Для демонстрації злому буде використано наступну схему (рис. 3.2), на якій зображено типову топологію мережі до початку проведення атаки зловмисником.

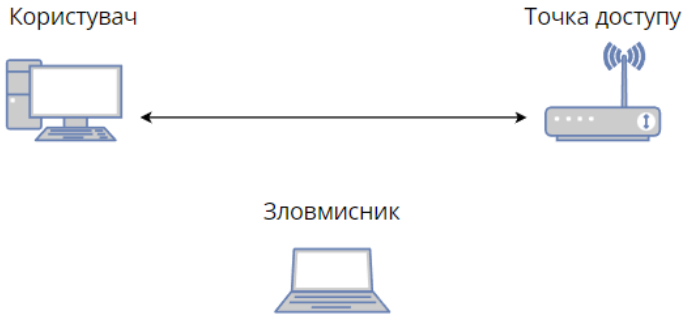

Рисунок 3.2 – Топологія мережі до початку атаки

Зловмисник має встановлену операційну систему Ubuntu 20.04, встановлений пакет aircrack-ng та зовнішній WiFi адаптер.

2. Відключення програм, які можуть мати вплив на роботу WiFi адаптера.

На рис. 3.3 зображено результат виконання команди *airmon-ng check kill*, яка видаляє процеси, які можуть мати вплив на роботу WiFi адаптера.

```
root@LW01-LHP-F72077:/home/bohdan# airmon-ng check kill

Killing these processes:

    PID Name
  17115 wpa_supplicant
```

Рисунок 3.3 – Відключення мережевих процесів

3. Переконфігурування WiFi адаптеру у режим моніторингу для перехоплення пакетів даних.

На рис. 3.4 зображено результат виконання команди *airmon-ng start <interface_name>*, яка переконфігуровує WiFi адаптер у режим моніторингу.

```
wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

Рисунок 3.4 – WiFi адаптер у режимі моніторингу

4. Сканування і вибір мережі для злому

Для демонстрації буде використано тестову точку доступу з SSID Test_AP.

На рис. 3.5 зображено результат виконання команди *airodump-ng wlan0mon*, яка запускає процес сканування.

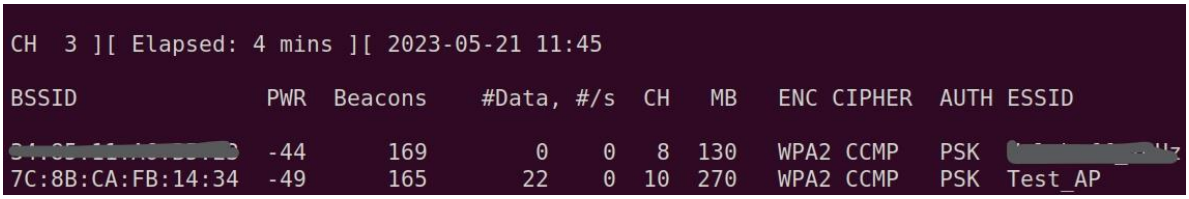

Рисунок 3.5 – Видимі під час сканування точки доступу

Під час сканування можна побачити MAC-адресу точки доступу, потужність сигналу, канал, на якому вона працює, тип шифрування і аутентифікації і її SSID.

5. Перехоплення пакетів чотирикратного рукостискання

Для перехоплення пакетів чотирикратного рукостискання потрібно спочатку налаштувати інтерфейс на прослуховування і запис пакетів у файл для однієї конкретної точки доступу. Це можна зробити насутпною командою *airodump-ng -w hack1 -c 10 --bssid <AP MAC-address> wlan0mon,* де опція *-w hack1* означає записування пакетів даних у файл під назвою *hack1, -c 10* значить канал, на якому працює точка доступу, дані від якої перехоплюються, *--bssid <AP MAC-address>* значить ім’я точки доступу. На рис. 3.6 зображено топологію мережі під час відключення клієнта зловмисником.

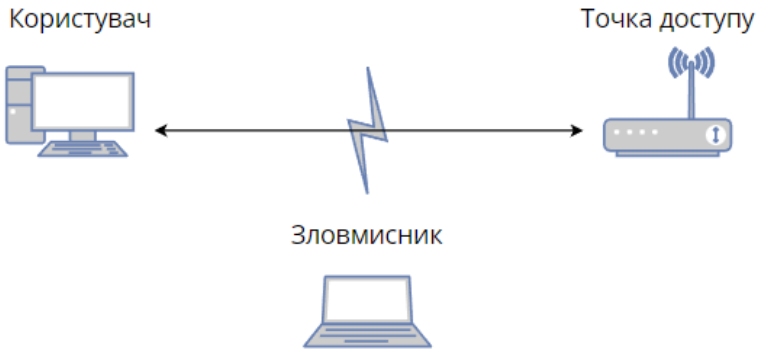

Рисунок 3.6 – Топологія мережі під час відключення клієнта

Так як процедура чотирикратного рукостискання відбувається тільки при аутентифікації користувача при під'єднанні, то, для пришвидшення отримання пакетів, треба від'єднати користувача від точки доступу на короткий термін часу і дочекатися його під'єднання.

Від'єднати користувача від точки доступу можна наступною командою *ariplay-ng --deauth 10 -a <AP MAC-address> -c <Client MAC-address> wlan0mon*, де *--deauth* опція означає процедуру відключення, 10 - канал, на якому працює точка доступу, *-a <AP MAC-address>* - MAC-адреса точки доступу, *-c <Client MAC-address>* - MAC-адреса клієнта, який буде відключений. На рис. 3.7 зображено процес відключення клієнта від точки доступу, а на рис. 3.8 зображено процес перехоплення пакетів 4-кратного рукостискання, яке відбувається паралельно відключенню клієнта.

```
bohdan@LW01-LHP-F72077:~$ sudo aireplay-ng --deauth 10 -a 7C:8B:CA:FB:14:34 -c B0:FC:36:AE:F9:8F wlan0mon
10:43:42  Waiting for beacon frame (BSSID: 7C:8B:CA:FB:14:34) on channel 10
10:43:43  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [30|63 ACKs]
10:43:43  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [78|68 ACKs]
10:43:44  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [64|60 ACKs]
10:43:44  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [64|69 ACKs]
10:43:45  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [54|61 ACKs]
10:43:45  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [65|60 ACKs]
10:43:46  Sending 64 directed DeAuth (code 7). STMAC: [B0:FC:36:AE:F9:8F] [60|58 ACKs]
^C
```

Рисунок 3.7 – Деаутентифікація клієнта

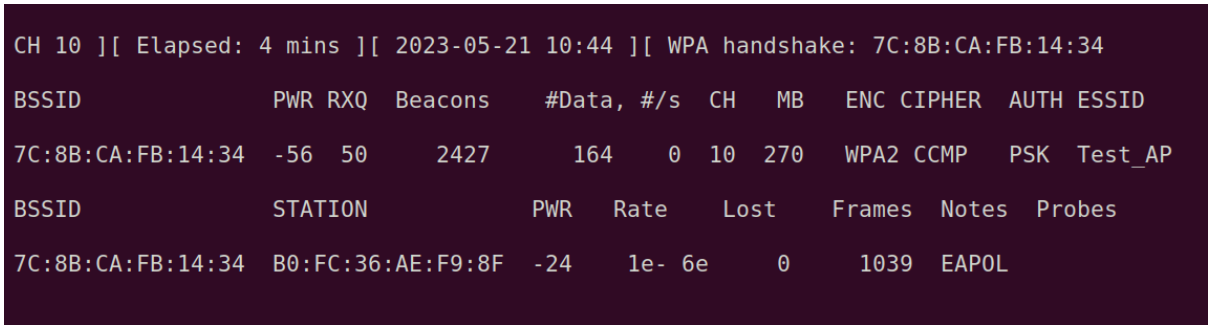

Рисунок 3.8 – Перехоплення пакетів 4-кратного рукостискання

При успішній деаутентифікації клієнта, у вікні моніторингу можна буде побачити *WPA handshake: <AP MAC-address>* . На рис. 3.7 зображені пакети 4-кратного рукостискання у програмі WireShark.

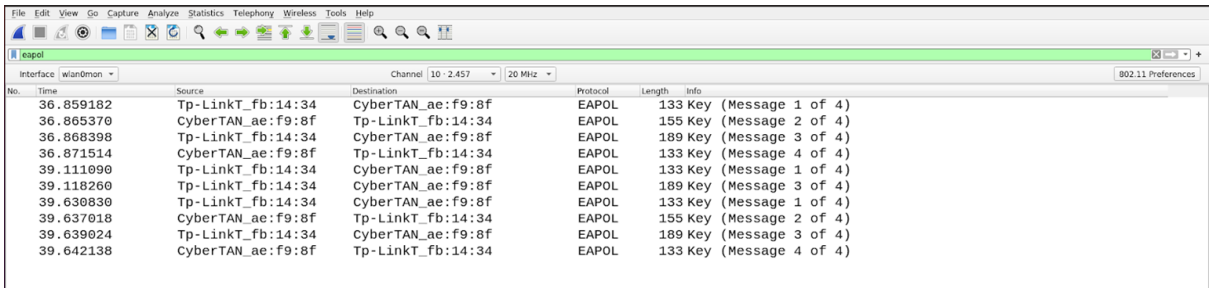

Рисунок 3.9 – Аналіз пакетів 4-кратного рукостискання у WireShark

Для того, щоб переконатися, що пакети з процедури чотирикратного рукостискання були успішно перехоплені і збережені у файл, достатньо відкрити файл *hack1.cap*, у який зберігалися дані за допомогою WIreShark і, застосовуючи фільтр eapol, проаналізувати наявність цих пакетів.

6. Перебір паролів зі словника паролів, або звичайним перебором комбінацій символів, цифр, знаків.

Після успішного отримання пакетів даних чотирикратного рукостискання можна починати підбір паролів за допомогою словника паролів *rockyou.txt*, який є у вільному доступі і містить порядка 15 млн. паролів.

Почати злом можна наступною командою *aircrack-ng hack1-01.cap -w rockyou.txt,* де *hack1-01.cap* - файл, що містить пакети чотирикратного рукостискання, *-w rockyou.txt* - словник паролів.

Під час виконання команди можна слідкувати за процесом злому, і, при знаходженні паролю, у терміналі буде виведено повідомлення *KEY FOUND! [<key>]*. На рис. 3.10 зображено вивід програми при успішному розшифруванні паролю.

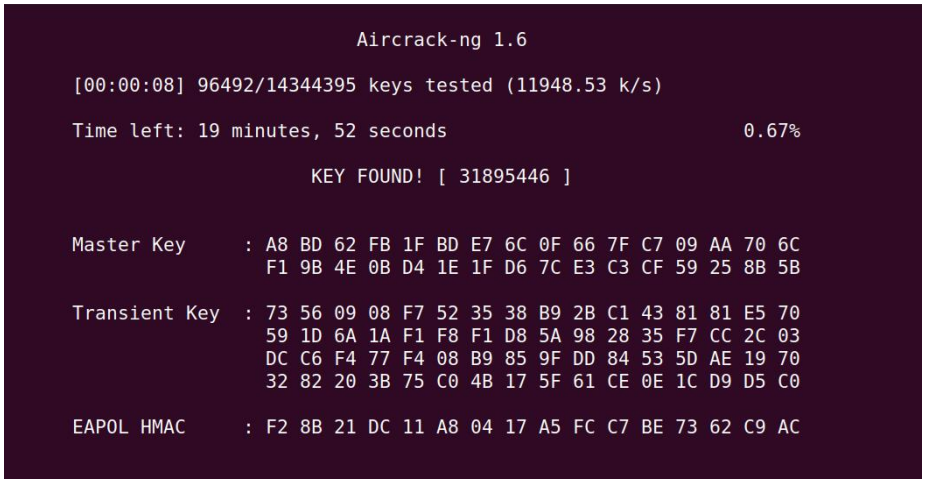

Рисунок 3.10 – Успішне отримання паролю

7. Підключення до точки доступу

Після отримання паролю точки доступу, зловмисник може вільно підключатися до неї і проводити подальші атаки, наприклад атака типу Man-In-The-Middle.

3.4 Мета злому

Після отримання доступу до мережі (у випадку, якщо мережа не є відкритою) зловмисник може застосувати так звану атаку Man In The Middle . Атаки "людина посередині" (Man-in-the-Middle Attacks): Ці атаки передбачають перехоплення комунікації між двома пристроями, що з'єднані

з бездротовою мережею, і маніпулювання або перехопленням передачі даних між ними. Зловмисник може перехопити, модифікувати або вставляти власні дані в комунікацію між пристроями. На рис. 3.11 зображено топологію мережі при успішній атаці типу “людина посередині”, де увесь трафік від пристрою користувача проходить через пристрій зловмисника.

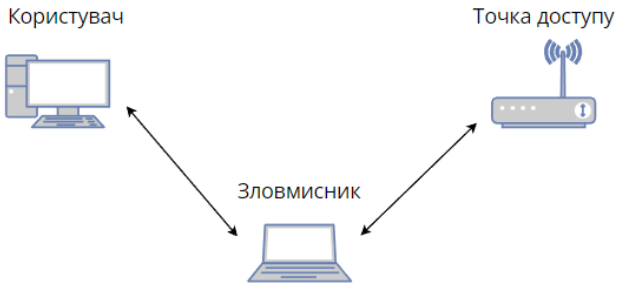

Рисунок 3.4.1 – Топологія мережі при успішній атаці типу “людина посередині”

4. Вимоги до пристрою і його функціонал

В сучасних умовах роботи, які часто потребують від користувачів взаємодії з потенційно небезпечними мережами важливо мати пристрій, який буде розділяти користувача від даної мережі і знижувати до мінімуму небезпеку від перебування в ній.

1. Пристрій повинен мати не менше двох окремих WiFi інтерфейсів, один з яких буде виступати у ролі клієнта для публічної мережі, а інший точкою доступа для клієнта.

2. Пристрій повинен мати принаймні один Ethernet інтерфейс, який може виступати у ролі роутера для користувача, а також використовуватися для налаштування пристрою

3. Пристрій повинен мати передвстановлений VPN клієнт

4. Пристрій повинен мати передвстановлений блокувальник реклами

5. Пристрій не повинен мати фільтр MAC адрес

6. WiFi інтерфейс пристрою , яки слугує точкою доступу для користувача не повинен працювати у режимі прихованої станції

7. Пристрій повинен за замовчуванням використовувати WPA3 або, принаймні, WPA2 аутентифікацію і вимагати від користувача використовувати пароль не менше 12 символів, який має складатися з комбінації букв нижнього та верхнього регістру, спеціальних символів та цифр.

4.1 Типовий спосіб використання

Пристрій призначений для забезпечення додаткового “шару” захисту користувача при використанні потенційно небезпечних мереж. На рис. 4.1 зображено топологію мережі при типовому використанні портативного роутера.

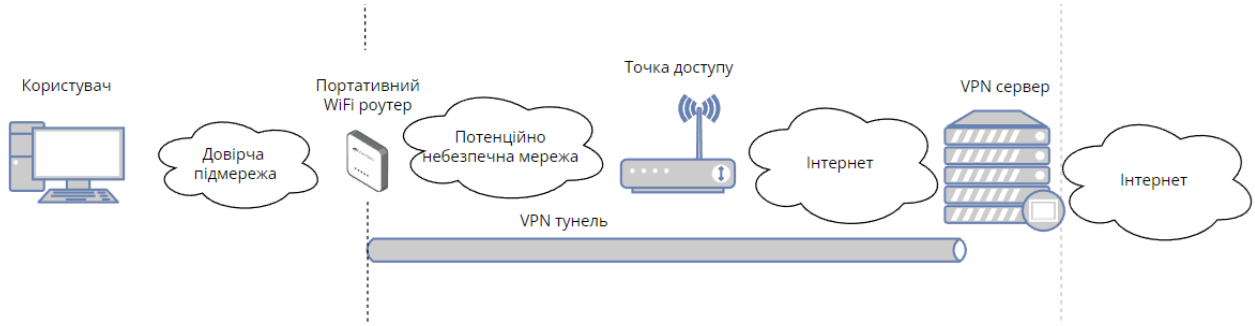

Рисунок 4.1.1 – Топологія мережі при типовому використанні портативного роутера

Пристрій має два безпровідних інтерфейса, одним з них підключається до публічної мережі, а інший слугує точкою доступу для користувача і

створює дві “зони”: пристрій-інтернет і користувач-пристрій.

Тобто фактично пристрій створює “довірчу” підмережу для користувача.

Пристрій має встановлений VPN клієнт, який створює віртуальний тунель і увесь трафік, який проходить з пристрою в інтернет, шифрується за допомогою протоколу використовуваного VPN (OpenVPN або Wireguard), тому спроба зловмисників провести атаку типу “людина посередині” і перехопити трафік не матиме сенсу, так як увесь трафік зашифрований, тому надалі зона пристрій-інтернет, при коректній роботі портативного роутера, вважатиметься такою, що не нестиме загрози персональним даним користувача. На рис. 4.2 зображено топологію мережі при спробі зловмисника перехопити дані, які проходять через VPN тунель.

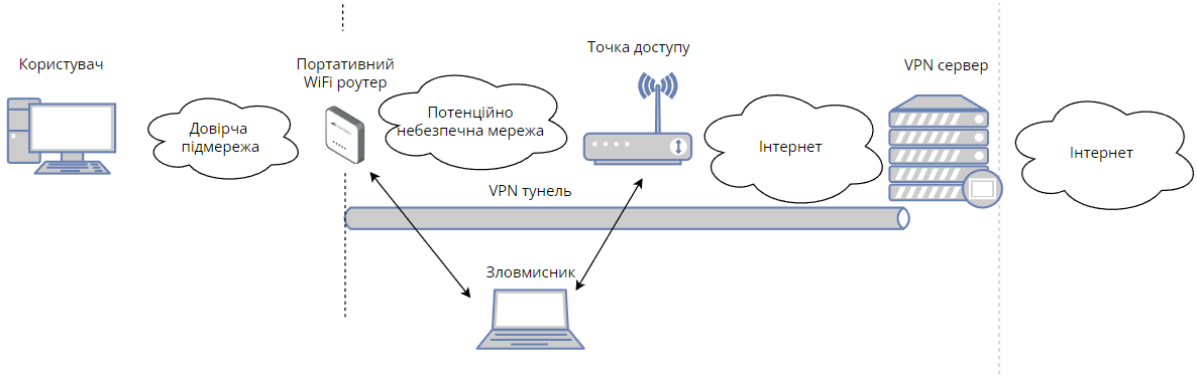

Рисунок 4.1.2 – Топологія мережі при спробі зловмисника перехопити дані, які проходять через VPN тунель

Зона користувач-пристрій використовує WPA3 або принаймні WPA2 типи аутентифікації, firewallб не використовує фільтрацію MAC адрес, має змінені стандартні IP і MAC адреси, заблокована можливість отримати доступ до пристрою через безпровідний інтерфейс, що у комбінації зі складним паролем (не менше 12 символів, який має складатися з комбінації букв нижнього та верхнього регістру, спеціальних символів та цифр),

нададуть достатній рівень захищеності пристрою від несанкціонованого доступу і перехоплення даних користувача. Також, задля підвищення захищеності користувача від загрози відвідування небезпечних веб-ресурсів на пристрої налаштований Adblocker і розроблені рекомендації використання і налаштування. На рис. 4.1 зображено топологію мережі при спробі зловмисника перехопити дані, які проходять між користувачем і портативним WiFi роутером.

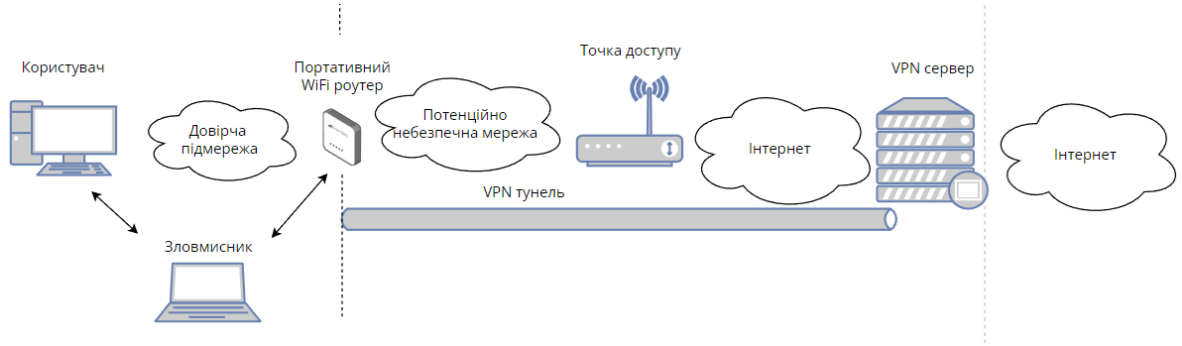

Рисунок 4.1.3 – Топологія мережі при спробі зловмисника перехопити дані, які проходять між користувачем і портативним WiFi роутером

ВИСНОВКИ

Публічні мережі дуже зручні для користування, так як надають можливість отримувати доступ до інтернету практично з будь-якого місця у будь-який час. Але, зважаючи на те, що ці мережі налаштовуються і контролюються невідомими користувачу особами, а також часто є відкритими, тобто не потребують аутентифікації та авторизації і будь-хто може приєднатися до подібної мережі і використовувати особливості і вразливості мережі, подібні мережі не можна вважати безпечними. Саме тому дуже важливим є забезпечення безпечного доступу до інтернету у даних мережах.

Тому для підвищення безпеки використання публічних WiFi мереж був розроблений концепт приладу, який має на меті відмежувати користувача від потенційно небезпечної частини мережі, і зменшити ризики втрати приватних даних. Також розглянуті основні вразливості різних типів шифрування та аутентифікації і інструменти їх злому, для розуміння того, на шо орієнтуватися, при розробці прототипу.

Список джерел і посилань

1) ІНСТРУМЕНТ АУДИТУ WiFi МЕРЕЖ [Електронний ресурс] // aircrack-ng.org. – 2023. – Режим доступу до ресурсу: https://www.aircrack-ng.org/

2) ІНСТРУМЕНТ ВІДНОВЛЕННЯ ПАРОЛІВ ЗА НАЯВНИМИ ХЕШАМИ [Електронний ресурс] // hashcat.net. – 2023. – Режим доступу до ресурсу: https://hashcat.net/

3) ІНСТРУМЕНТ МОНІТОРИНГУ СЕРЕДОВИЩА БЕЗПРОВІДНОЇ ПЕРЕДАЧІ ДАНИХ [Електронний ресурс] // kismetwireless.net. – 2023. – Режим доступу до ресурсу: https://www.kismetwireless.net/

4) АЛГОРИТМИ АУТЕНТИФІКАЦІЇ І ШИФРУВАННЯ WiFi МЕРЕЖ [Електронний ресурс] // securew2.com – 2020. – Режим доступу до ресурсу: https://www.securew2.com/blog/complete-guide-wi-fi-security

5) БЕЗПЕКА WiFi МЕРЕЖ [Електронний ресурс] // techtarget.com – 2022. – Режим доступу до ресурсу https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2